Filed for intro on 02/13/2003
HOUSE BILL 782 By
Patton

SENATE BILL 1085
By Jackson

AN ACT to enact the Tennessee Personal and Commercial Computer Act of 2003.

BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF TENNESSEE:

SECTION 1. This act shall be known and may be cited as the "Tennessee Personal and Commercial Computer Act of 2003".

SECTION 2. As used in this act, unless the context otherwise requires:

(1) "Access" means to approach, instruct, communicate or connect with, store data in, retrieve or intercept data from, or otherwise make use of any resources of a computer, computer system or computer network, or information exchanged from any communication between computers or authorized computer users and electronic, electromagnetic, electrochemical, acoustic, mechanical, or other means;

(2) "Computer" means a device or collection of devices, including its support devices or peripheral equipment or facilities, and the communication systems connected to it which can perform functions including, but not limited to, substantial computation, arithmetic or logical operations, information storage or retrieval operations, capable of being used with external files, one (1) or more

operations which contain computer programs, electronic instructions, allows for the input of data, and output data (such operations or communications can occur with or without intervention by a human operator during the processing of a job);

(3) "Computer contaminants" means any set of computer instructions that are designed to modify or in any way alter, damage, destroy, or disrupt the proper operation of a computer system, or computer network without the intent or permission of the owner of the information. They include, but are not limited to, a group of computer instructions commonly called viruses or worms, which are self-replicating or self-propagating and are designed to contaminate other computer programs or computer data, consume computer resources, modify, destroy, record or transmit data, or in some other fashion usurp the normal operation of the computer, computer system, or computer network. Such contaminants may include:

(A) "Virus" meaning a migrating program which, at least, attaches itself to the operating system of any computer it enters and can infect any other computer that has access to an "infected" computer; and

(B) "Worm" meaning a computer program or virus that spreads and multiplies, eventually causing a computer to "crash" or cease functioning, but does not attach itself to the operating system of the computer it "infects";

(4) "Computer network" means a set of two (2) or more computer systems that transmit data over communication circuits connecting them, and input/output devices including, but not limited to, display terminals and printers, which may also be connected to telecommunication facilities;

(5) "Computer program" means an ordered set of data that are coded instructions or statements that, when executed by a computer, cause the computer to process data;

(6) "Computer software" means a set of computer programs, procedures, and associated documentation concerned with the operation of a computer, computer system, or computer network whether imprinted or embodied in the computer in any manner or separate from it, including the supporting materials for the software and accompanying documentation;

(7) "Computer system" means a set of connected devices including a computer and other devices including, but not limited to, one (1) or more of the following: data input, output, or storage devices, data communication circuits, and operating system computer programs that make the system capable of performing data processing tasks;

(8) "Data" means a representation of information, knowledge, facts, concepts, or instructions which is being prepared or has been prepared in a formalized manner, and is intended to be stored or processed, or is being stored or processed, or has been stored or processed, in a computer, computer system, or computer network;

(9) "Electronic mail service provider" means any person who:

(A) is an intermediary in sending or receiving electronic mail; and

(B) provides to end-users of electronic mail services the ability to send or receive electronic mail;

(10) "Financial instrument" includes, but is not limited to, any check, cashier's check, draft, warrant, money order, certificate of deposit, negotiable instrument, letter of credit, bill of exchange, credit card, debit card, marketable security, or any computer system representation thereof;

(11) "Input" means data, facts, concepts or instructions in a form appropriate for delivery to, or interpretation or processing by, a computer;

(12) "Intellectual property" includes data, which may be in any form including, but not limited to, computer printouts, magnetic storage media, punched cards, or may be stored internally in the memory of a computer;

(13) "Output" means data, facts, concepts or instructions produced or retrieved by computers from computers or computer memory storage devices;

(14) "Owner" means an owner or lessee of a computer or a computer network or an owner, lessee or licensee of computer data, computer programs, or computer software;

(15) "Property" shall include:

(A) real property;

(B) computers and computer networks;

(C) financial instruments, computer data, computer programs, computer software, and all other personal property regardless of whether they are:

(i) tangible or intangible;

(ii) in a format readable by humans or by a computer;

(iii) in transit between computers or within a computer network or between any devices which comprise a computer; or

(iv) located on any paper or in any device in which it is stored by a computer or by a human;

(16) "To process" means to use a computer to put data through a systematic sequence of operations for the purpose of producing a specified result;

(17) "Services" includes, but is not limited to, the use of a computer, a computer system, a computer network, computer software, computer program or data to perform tasks; and

(18) "System hacker" means any person who knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network.

SECTION 3.

(a) Whoever knowingly, directly or indirectly, accesses, causes to be accessed, or attempts to access any telephone system, telecommunications facility, computer software, computer program, data, computer, computer system, computer network, or any part thereof, for the purpose of:

(1) Obtaining money, property, or services for oneself or another by means of false or fraudulent pretenses, representations, or promises violates this subsection and is subject to the penalties of § 39-14-105;

(2) Causing computer output to purposely be false, for, but not limited to, the purpose of obtaining money, property, or services for oneself or another by means of false or fraudulent pretenses, representations, or promises violates this subsection and is subject to the penalties of § 39-14-105; or

(3) Effecting the creation or alteration of a financial instrument or of an electronic transfer of funds violates this subsection and is subject to the penalties of § 39-14-105.

(b) Whoever intentionally and without authorization, directly or indirectly:

(1) Accesses any computer, computer system, or computer network commits a Class C misdemeanor;

(2) Alters, damages, destroys, or attempts to damage or destroy, or causes the disruption to the proper operation of any computer, or who performs

an act which is responsible for the disruption of any computer, computer system, computer network, computer software, program or data which resides or exists internal or external to a computer, computer system, or computer network is punishable as in § 39-14-105;

(3) Introduces or is responsible for the input of any computer contaminant into any computer, computer system, or computer network commits a Class B misdemeanor;

(4) Accesses, causes to be accessed, or attempts to access any computer software, computer program, data, computer, computer system, computer network, or any part thereof, for the purpose of gaining access to computer material or to tamper with computer security devices, including, but not limited to, system hackers, commits a Class A misdemeanor; or

(5) Makes or causes to be made an unauthorized copy, in any form, including, but not limited to, any printed or electronic form of computer data, computer programs or computer software residing in, communicated by, or produced by a computer or computer network commits an offense punishable as provided in § 39-14-105.

(c) Whoever receives, conceals, uses, or aids another in receiving, concealing, or using any proceeds resulting from a violation of either subsection (a) or subdivision (b)(2), knowing the same to be proceeds of such violation, or whoever receives, conceals, uses, or aids another in receiving, concealing, or using, any books, records, documents, property, financial instrument, computer software, program, or other material, property, or objects, knowing the same to have been used in violating either subsection (a) or subdivision (b)(2) is subject to the penalties of § 39-14-105.

SECTION 4.

(a) It is an offense for a person without authority to falsify or forge electronic mail transmission information or other routing information in any manner in connection with the transmission of unsolicited bulk electronic mail through or into the computer network of an electronic mail service provider or its subscribers.

(b) Transmission of electronic mail from an organization to its members shall not be deemed to be the transmission of unsolicited bulk electronic mail as prohibited by this section.

(c) Nothing in this section shall be construed to interfere with or prohibit terms or conditions in a contract or license related to computers, computer data, computer networks, computer operations, computer programs, computer services, or computer software or to create any liability by reason of terms or conditions adopted by or technical measures implemented by a Tennessee-based electronic mail service provider to prevent the transmission of unsolicited electronic mail in violation of this act.

(d) As used in this section, "without authority" means a person uses a computer, a computer network, or the computer services of an electronic mail service provider to transmit unsolicited bulk mail in contravention of the authority granted by or in violation of the policies set electronic by the electronic mail service provider.

(e) A violation of this section shall be punished according to the damage to the property of another caused by the violation and shall be graded as provided in § 39-14-105.

SECTION 5.

(a) Any person whose property or person is injured by reason of a violation of any provision of this act may file a civil action and recover for any damages sustained and the costs of the civil action. Without limiting the generality of the term, "damages" shall include loss of profits.

(b) If the injury arises from the transmission of unsolicited bulk electronic mail, the injured person, other than an electronic mail service provider, may also recover attorney's fees and costs, and may elect, in lieu of actual damages, to recover the lesser of ten dollars ($10.00) for each and every unsolicited bulk electronic mail message transmitted in violation of this act, or one thousand dollars ($1,000) per day. The injured person shall not have a cause of action against the electronic mail service provider that merely transmits the unsolicited bulk electronic mail over its computer network.

(c) If the injury arises from the transmission of unsolicited bulk electronic mail, an injured electronic mail service provider may also recover attorney's fees and costs and may elect, in lieu of actual damages, to recover the greater of ten dollars ($10.00) for each and every unsolicited bulk electronic mail message transmitted in violation of this article, or one thousand dollars ($1,000) per day.

(d) At the request of any party to an action brought pursuant to this section, the court may, in its discretion, conduct all legal proceedings in such a way as to protect the secrecy and security of the computer, computer network, computer data, computer program, and computer software involved in order to prevent possible recurrence of the same or a similar act by another person and to protect any trade secrets of any party. The provisions of this section shall not be construed to limit any person's right to pursue any additional civil remedy otherwise allowed by law.

SECTION 6. For the purposes of venue under the provisions of this part, any violation of this part shall be considered to have been committed:

(1) In any county in which any act was performed in furtherance of any transaction violating this part;

(2) In any county in which any violator had control or possession of any proceeds of the violation or of any books, records, documents, property, financial

instrument, computer software, computer program, or other material, objects, or items which were used in furtherance of the violation; and

(3) In any county from which, to which or through which, any access to a computer, computer system, or computer network was made, whether by wire, electromagnetic waves, microwaves, or any other means of communication.

SECTION 7. The Tennessee code commission is directed to codify the provisions of this act in place of existing Tennessee Code Annotated, Title 39, Chapter 14, Part 6.

SECTION 8. This act shall take effect July 1, 2003, the public welfare requiring it.